WACIRC
Law Enforcement Guidelines for Reporting and Responding to Computer Crimes

Version 1.7

Contact the WSP Computer Crimes Unit to report a computer crime within a State Agency

360-753-6800

Table of Contents

Intended Audience 2
Expected Benefits 2
Introduction 3
Types of Computer Crimes Covered by these Guidelines 4
Law Enforcement Contact Decision Matrix 6
Evidence Chain of Custody Guidelines 7
Required Actions: 7
Guiding Principles: 7
WSP Computer Crime Response Procedure 8
Phase 1: Information Gathering – (WSP Checklist) 8
Phase 2: Incident Assessment 9
Phase 3: Law Enforcement Response 9
WSP Guideline & Jurisdictional Directive 11

Intended Audience

The intended audience for this document is individuals in state agencies who are responsible for managing and operating computer systems.

Expected Benefits

- A process that is easy to incorporate into the agency's Computer Incident Response Procedures.
- Guidelines that form the basis for a common understanding of computer related crimes
- Specific actions that should be taken by agency management and staff when a computer related crime is suspected.
- Reduced time for agencies to get the right law enforcement people involved in a computer crime investigation.
- A clear outline of the roles and responsibilities an Agency and the WSP during a computer crime investigation.

Introduction

Currently there is no consistent and broadly understood way for State Agency security or Information Technology (IT) professionals to contact Law Enforcement agencies in a time effective way. Recent incidents suggest that the needs of Law Enforcement are not well understood by the IT community nor are the needs of the IT Community well understood by Law Enforcement.

A sub-committee chartered by the Washington State Computer Incident Response Center (WACIRC) addressed this problem. The sub-committee included individuals from the Washington State Patrol (WSP) Investigative Assistance Division (IAD), the Attorney General's (ATG) high-tech crimes unit and WACIRC representatives from other state agencies. The sub-committee has recommended improved procedures with WSP and has developed a set of guidelines to be used when all agencies and their IT management teams suspect a crime.

The WSP procedures and IT Guidelines were reviewed and approved by WSP management, ATG management, the WACIRC Steering Committee, and the Department of Information Services (DIS) Enterprise Security Manager.

Our goal in preparing these guidelines was to develop a consistent process to be used by all agencies when a computer crime has occurred or is suspected. The key feature of these guidelines is that all agencies now have a single point of contact to ask for help or report a criminal incident to law enforcement. In the past, jurisdictional challenges within the law enforcement community complicated the issue of who to call. The WSP has worked with other law enforcement entities statewide to implement a clear understanding that WSP will be the lead investigating agency for computer crimes within State Agencies.

WACIRC Law Enforcement Subcommittee Members

Andrea Powell	ATG	586-3631	andreap@atg.wa.gov
Lana Weinmann	ATG	206-389-2022	lanam@atg.wa.gov
Dan Husmann	DIS	902-3306	danh@dis.wa.gov
Cliff Schiller	DOH	236-4432	cliff.schiller@doh.wa.gov
Amy Ridgeway	HCA	923-2845	aridl07@hca.wa.gov
Doug Selix	OFM	902-0574	doug.selix@ofm.wa.gov
Keith Huntley	WSP	753-6800	khuntle@wsp.wa.gov
Jesse Regalado	WSP	753-6800	jregalado@wsp.wa.gov
Tracy Dike	WSP	705-5158	tdike@wsp.wa.gov

Types of Computer Crimes Covered by these Guidelines

The types of crimes listed below determine the scope of these guidelines.

1. **Computer Trespass**

   Definitions:

   - Computer Trespass in the first degree (class C felony) RCW 9A.52.110 – the unauthorized, intentional access to a computer system or electronic data base of another with either:

     (1) the intent to commit another crime; or

     (2) the violation involves a comp uter or data base maintained by a government agency.

   - Computer Trespass in the second degree (gross misdemeanor) RCW 9A.52.120 - the unauthorized, intentional access to a computer system or electronic data base of another that does not amount to a computer trespass in the first degree.

   Examples:

   - **Unauthorized access to a computer or network** – Someone, without authorization, accesses a particular government computer system. The access alone, without the intent to commit another crime, can be a felony.
   - **Inappro priate use of a computer or network –** An employee of the agency, who has authorized access to the computer system, but who abuses that privilege and uses their access for unauthorized purpose. This may not amount to a computer trespass, but a report should be made to determine whether any other crime has been committed.

2. **Extortion**

   Definition (RCW 9A.56.110, 120, 130)**:**

   - Obtaining or attempting to obtain property or services by means of a threat. This can include a threat to expose a secret or a fact.

   Examples:

   - **Threat to data integrity** – a suspect threatens to destroy or alter data to obtain something of value.
   - **Threat of data or information release** – a suspect claims to have obtained access to agency data or other information and threatens to reveal the security breach if not provided with money or other things of value.

3. **Malicious Mischief**

   Definitions:

   Knowingly and maliciously causing physical damage to the property of another in the following amounts or manners:

   (1) First degree (class B felony) RCW 9A.48.070

   (a) Causes damage in excess of $1500; or

   (b) Causes an interruption or impairment of service rendered to the public by physically damaging or tampering with property of the state, a political subdivision thereof, or a public utility or mode of public transportation, power, or communication.

   (2) Second degree (class C felony) RCW 9A.48.080

(a) Causes physical damage to the property of another in excess of $250, but not more than $1,500; or
(b) Creates a substantial risk of interruption or impairment of service rendered to the public, by physically damaging or tampering with property of the state, a political subdivision thereof, or a public utility or mode of public transportation, power, or communication.

(3) Third degree; RCW 9A.48.090
(a) Physical damage in excess of $50 is a gross misdemeanor;
(b) Physical damage under $50 is a misdemeanor.

Note: "Physical damage", in addition to its ordinary meaning, shall include the total or partial alteration, damage, obliteration, or erasure of records, information, data, computer programs, or their computer representations, which are recorded for use in computers or the impairment, interruption, or interference with the use of such records, information, data, or computer programs, or the impairment, interruption, or interference with the use of any computer or services provided by computers. "Physical damage" also includes any diminution in the value of any property as the consequence of an act.

Examples:

- **Malicious code attacks** (virus, virus hoaxes, worm, etc.)
- **Denial of service attacks** – disrupting a computer or network.
- **Alteration or destruction of agency data**

4. Theft

Definitions (RCW 9A.56.020**):**

"Theft" means:

(a) To wrongfully obtain or exert unauthorized control over the property or services of another or the value thereof, with intent to deprive them of such property or services; or

(b) By color or aid of deception (e.g. trickery) to obtain control over the property or services of another or the value thereof, with intent to deprive them of such property or services; or

(c) To appropriate lost or misdelivered property or services of another, or the value thereof, with intent to deprive them of such property or services.

Degrees:

(1) First degree (class B felony) RCW 9A.56.030 – value of property exceeds $1500.

(2) Second degree (class C felony) RCW 9A.56.040 – value of property exceeds $250, but is not more than $1500; or the property is a public record, writing, or instrument kept, filed, or deposited according to law with or in the keeping of any public office or public servant; or an access device.

(3) Third degree (gross misdemeanor) RCW 9A.56.050 – value of property is $250 or less.

Examples:

- **Theft of data or intellectual property**
- **Theft of physical computer equipment** ***– this area will likely be investigated by local police***, but if the computer equipment contained information that may give raise to any other potential crime, a report should be made through WACIRC.

5. **Server or computer being used to house evidence of a crime**

   IT Security personnel may discover that their server or computer(s) are being used to house evidence of other crimes. In those situations, steps should be taken to preserve the integrity of the evidence (see WACIRC Incident Handling Guidelines) and a report should be made to local law enforcement.

   Primary Examples: Child pornography, Threats or Harassment, Theft, Embezzlement or Fraud

6. **Probes and Network Mapping –** These are not crimes and should be investigated internally.

Law Enforcement Contact Decision Matrix

The table below is presented as an aid to help IT professionals and their management determine who to contact for each type of crime.

To contact WSP, call (360)-753-6800 and ask for the Computer Crimes Unit

Type of Incident	Who to contact						What to do			
	Agency Network Admin	Data or System Owner	Agency Management	DIS Helpdesk (Alert WACIRC)	Local Law Enforcement	WSP	Follow WSP Checklist	Document the Incident	Follow WACIRC Best Practice	Maintain Chain of Custody
Computer Trespass										
• **Unauthorized access to a computer or network**	X		X	WSP & Agency will determine if notification is appropriate		X	X	X	X	X
• **Inappropriate use of a computer or network**	X		X			X	X	X	X	X
Extortion										
• **Threat to data integrity**	X	X	X	WSP & Agency will determine if notification is appropriate		X	X	X	X	X
• **Threat of data or information release**	X	X	X			X	X	X	X	X
Malicious Mischief										
• **Malicious code attacks** (virus, worm, etc.)	X		X	X		Contact WSP only if you suspect this attack is localized to your agency. If it is a national attack, do not contact WSP			X	
• **Denial of service attacks** – disrupting a computer or network..	X		X	X					X	
• **Alteration of destruction of agency data**	X	X	X	X					X	
Theft										
• **Theft of data or intellectual property through electronic means**	X	X	X	WSP & Agency will determine if notification is appropriate		X	X	X	X	X
• **Theft of physical computer equipment**	X	X	X		X			X	X	X
Server or computer being used to house evidence of a crime	X	X	X		X	X	X	X	X	X
NOTE: Privacy related issues should be directed to your Agency Privacy Officer, Public Disclosure Officer or other appropriate Agency Management										

Evidence Chain of Custody Guidelines

When a crime is suspected it is important to preserve evidence. Courts have set very high standards for the proper handling of electronic and paper based evidence. Below are recommendations for proper handling of evidence.

Required Actions:

1. Contact the Washington State Patrol Computer Crimes Unit at (360) 753-6800 as soon as possible.
2. WSP instructions may include the following:
   a. Identify the agency person to who will be the WSP contact and the person, when directed by WSP, will control evidence.
   b. Ensure Evidence Custodian has secure area/container to secure evidence
   c. Identify potential pieces of evidence when event occurs
   d. Preserve all applicable system logs
   e. Collect identifying information (e.g. locations, serial numbers, etc.)
   f. Remove and seal suspected disk drives as evidence.
   g. Record all identifying information about suspect disk drives
   h. Preserve relevant backup data
   i. Make copies for continued operations and seal originals for evidence. Copies are not suitable for evidence.
   j. Number, data and sign any notes or hardcopy records that may be considered evidence.
   k. Sealed evidence should be in envelopes or some other container that can be sealed; the seals should be numbered, dated and signed by the person who sealed them.
   l. A log of all evidence should be kept. The log should have signatures and time controls recording every time evidence changes hands.
   m. Make sure that there is a witness for every chain of custody event. The witness should sign any logs or seals.

Guiding Principles:

1. Follow the WACIRC Computer Crime Incident Response Process.
2. If you suspect a crime, get your management and WSP involved as soon as possible.
3. WSP has the greatest knowledge and skill in preserving the value of computer related evidence. Only WSP should make decisions concerning appropriate handling of evidence.
4. Attempting to handle evidence on your own, even if well meaning, could taint the evidence and make it unusable for law enforcement purposes. Let WSP determine what to do with the evidence.
5. Be prepared--Have an "Incident Response Plan" that includes assigning someone to be the "evidence custodian". This person will work under the direction of WSP investigators to handle and control evidence during an investigation. This person should be the agency liaison with WSP.
6. Don't delete anything!

WSP Computer Crime Response Procedure

Phase 1: Information Gathering – (WSP Checklist)

- Date & Time of complaint (record time complaint received)
- Nature of incident (e.g. intrusion, Denial of Service (DOS) attack, Virus, email issue, theft of services, etc. provide detailed description)
- List any changes to victim system by staff at or after the incident was discovered (e.g. password file updates, log files preserved, firewall filter patches implemented, etc.)
- Person who discovered the incident and their functional relationship to the victim system
- Is victim system currently online/connected to the Internet?
- Is victim system still operational?
- Reporting party name and contact information
- Reporting party organization/business name and contact information
- List all persons who are working on the incident and their contact information
- Victim organization/business nature of business or function (what do they do, their product)
- Victim management chain (who's the boss that can make decisions?)
- Who is the lead system administrator of the victim system?
- Names of all other system administrators assigned to victim system
- Nature of system network (e.g. LAN, WAN, etc.)
- Victim system hostname
- Victim system IP address range assignments
- Victim system configuration design document
- Victim system architecture (e.g. IBM, Win2K, etc.)
- Victim system backup retention and availability
- Victim system data sensitivity (example: personnel information, financial, gateway access.)
- Logs indicating source of incident.
- Notification to WSP of any information contained in controlled evidence that cannot be disclosed under state law (e.g. information exempt from disclosure under RCW 42.17.310).

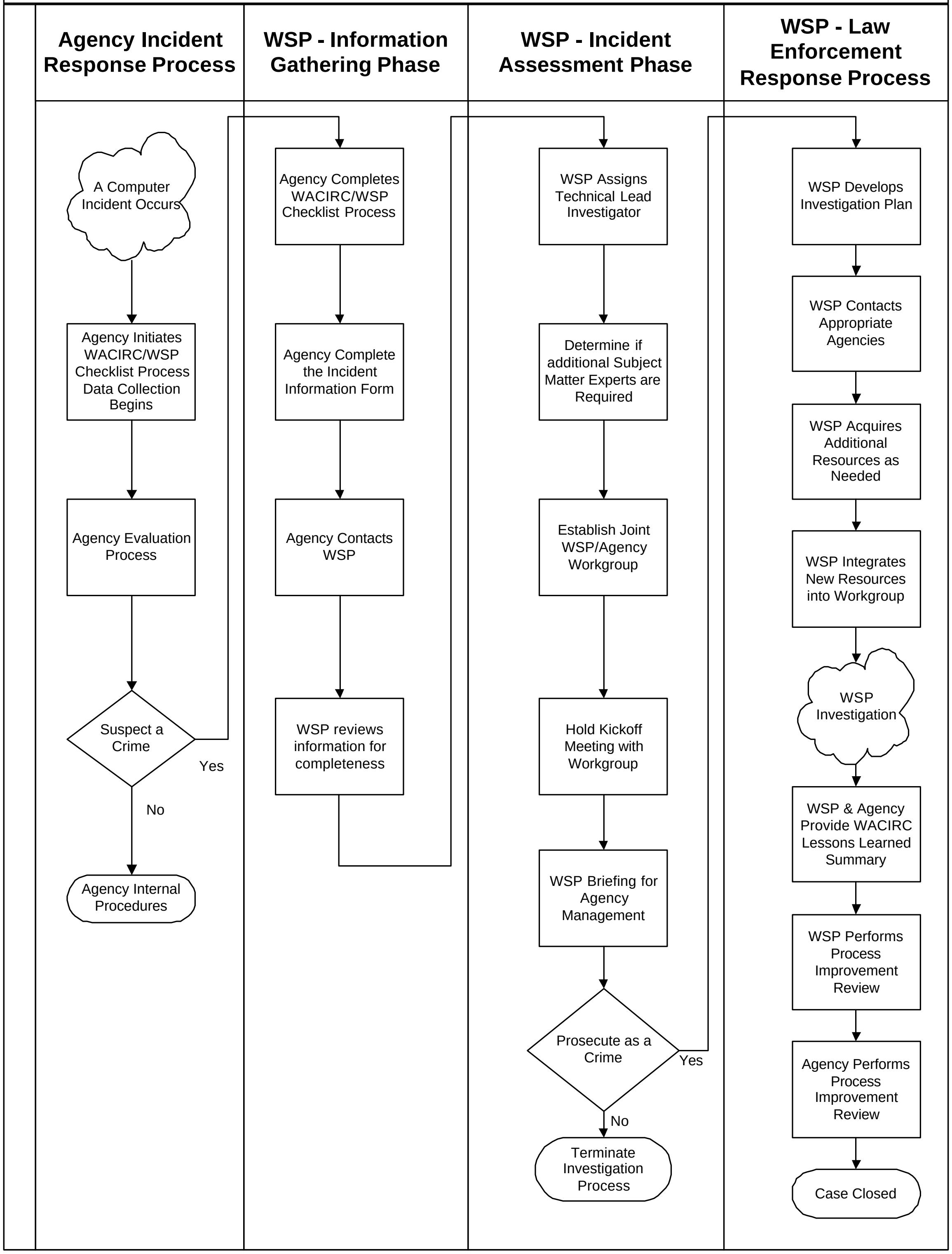
Phase 2: Incident Assessment

- Assign agency lead technical investigator responsible for WSP interface.
- Determine what technical subject matter experts are needed (e.g. Win2k administrators, firewall, administrators, network specialist, computer forensic specialist etc.) to assist the investigation.
- Form a workgroup to identify tasks and responsibilities.
- Establish a kickoff meeting to consolidate efforts between the Agency and WSP. This is the time for WSP to establish ground rules (e.g. roles, responsibilities, chain of custody tasks, etc.) and to meet with agency experts to initiate the investigation.
- Meet with victim management to identify best solution for the response.
    - Does the victim want to prosecute?
    - How much down time can the victim afford?
    - How much publicity about the incident will the victim be able to cope with?
    - Have the victim determine whether to continue the investigation or resolve the incident without further Law Enforcement involvement.
- A joint (WSP and Agency) decision will be made whether to initiate a Law Enforcement Response.

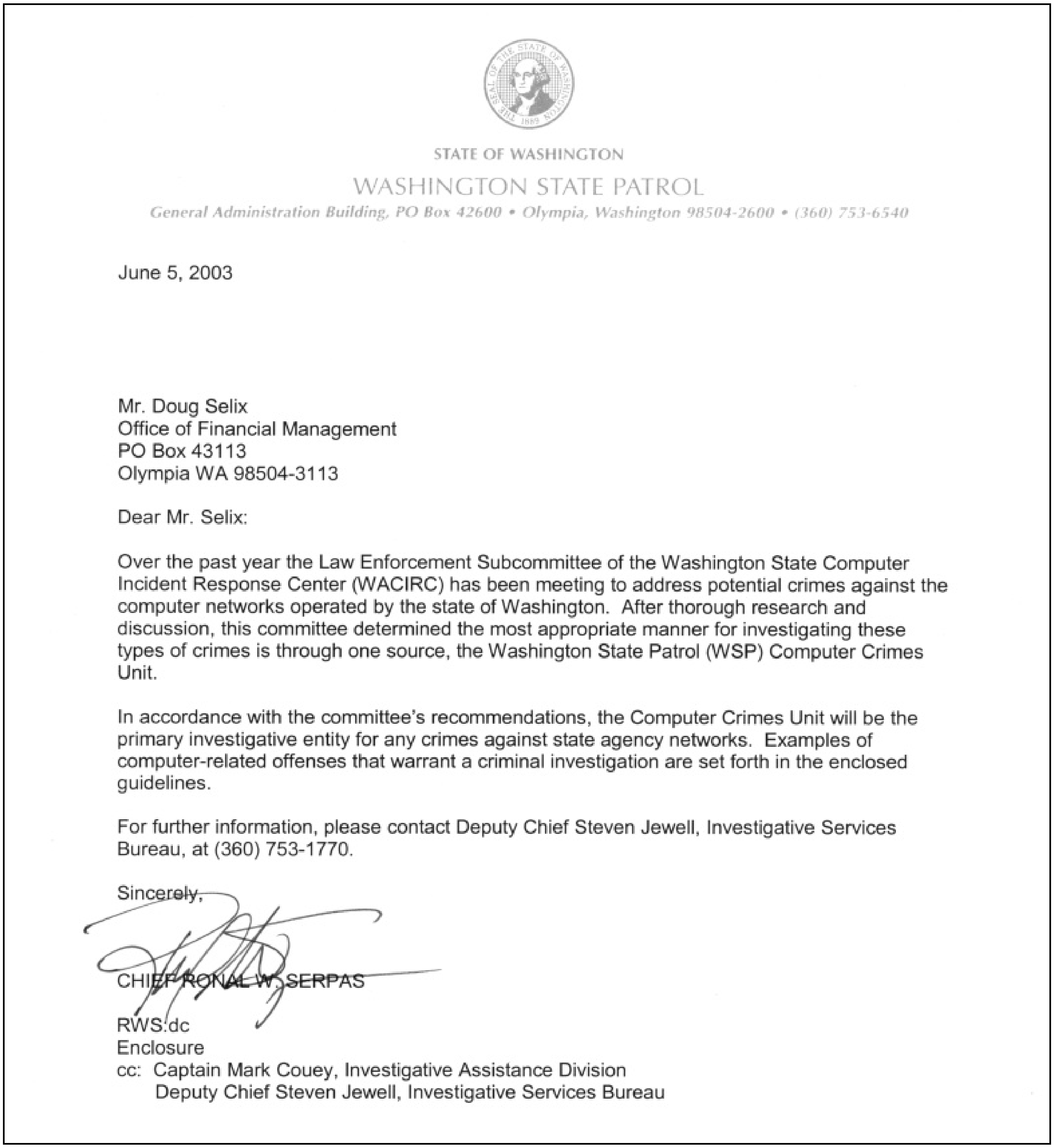
Phase 3: Law Enforcement Response

- WSP will develop the investigation plan
- WSP will contact appropriate local law enforcement and prosecutorial agencies
- WSP will identify and gather additional necessary resources to execute the investigation plan
- Review plan with additional resources and make necessary adjustments.
- WSP will critique incident and response plan, make necessary adjustments to improve future responses
- WSP and Agency will provide a “Lessons Learned” document to WACIRC for distribution to all WACIRC members.

WSP - Computer Incident Response Process


Agency Incident Response Process
WSP - Information Gathering Phase
WSP - Incident Assessment Phase
WSP - Law Enforcement Response Process
A Computer Incident Occurs
Agency Initiates WACIRC/WSP Checklist Process Data Collection Begins
Agency Evaluation Process
Suspect a Crime
Yes
No
Agency Internal Procedures
Agency Completes WACIRC/WSP Checklist Process
Agency Complete the Incident Information Form
Agency Contacts WSP
WSP reviews information for completeness
WSP Assigns Technical Lead Investigator
Determine if additional Subject Matter Experts are Required
Establish Joint WSP/Agency Workgroup
Hold Kickoff Meeting with Workgroup
WSP Briefing for Agency Management
Prosecute as a Crime
Yes
No
Terminate Investigation Process
WSP Develops Investigation Plan
WSP Contacts Appropriate Agencies
WSP Acquires Additional Resources as Needed
WSP Integrates New Resources into Workgroup
WSP Investigation
WSP & Agency Provide WACIRC Lessons Learned Summary
WSP Performs Process Improvement Review
Agency Performs Process Improvement Review
Case Closed

WSP Guideline & Jurisdictional Directive



STATE OF WASHINGTON

WASHINGTON STATE PATROL

General Administration Building, PO Box 42600 • Olympia, Washington 98504-2600 • (360) 753-6540

June 5, 2003

Mr. Doug Selix
Office of Financial Management
PO Box 43113
Olympia WA 98504-3113

Dear Mr. Selix:

Over the past year the Law Enforcement Subcommittee of the Washington State Computer Incident Response Center (WACIRC) has been meeting to address potential crimes against the computer networks operated by the state of Washington. After thorough research and discussion, this committee determined the most appropriate manner for investigating these types of crimes is through one source, the Washington State Patrol (WSP) Computer Crimes Unit.

In accordance with the committee's recommendations, the Computer Crimes Unit will be the primary investigative entity for any crimes against state agency networks. Examples of computer-related offenses that warrant a criminal investigation are set forth in the enclosed guidelines.

For further information, please contact Deputy Chief Steven Jewell, Investigative Services Bureau, at (360) 753-1770.

Sincerely,

CHIEF RONAL W. SERPAS

RWS:dc
Enclosure
cc: Captain Mark Couey, Investigative Assistance Division
Deputy Chief Steven Jewell, Investigative Services Bureau